Claims:

1. (Currently Amended) A method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second trusted time and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

2. (Original) The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key.

3. (Original) The method according to claim 2, wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion.

4. (Original) The method according to claim 2, wherein each of the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys.

5. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, performing a transaction between the first card and the second card.

6. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the verification fails, suspending a transaction between the first card and the second card.

7. (Original) The method according to claim 1, further comprising the step of:

if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device.

8. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first sequence number and the second sequence number are equal, performing a transaction between the first card and the second card.

9. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, wherein the setting step is performed by transmitting an authenticated system message ("ASM") command from the second card to the first card, and wherein at least one of the first and second cards sets the second sequence number.

10. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and wherein the first storage device stores a third sequence number thereon, wherein the second storage device stores a fourth sequence number thereon, and further comprising the steps of:

if the first sequence number and the second sequence number are equal, determining whether the third sequence number corresponds to the fourth sequence number; and

if the third sequence number does not correspond to the fourth sequence number, transmitting an authenticated system message ("ASM") command from a particular card of the first and second cards having a newer number of the third and fourth sequence numbers to another card of the first and second cards.

11. (Original) The method ac cording to claim 10, wherein the ASM command is transmitted without setting the first sequence number to have the value of the second sequence number.

12. (Original) The method according to claim 10, further comprising the step of:

if the third sequence number corresponds to the fourth sequence number, performing a transaction between the first card and the second card.

13. (Original) The method ac cording to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number.

14. (Original) The method ac cording to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device.

15. (Original) The method ac cording to claim 1, wherein each of the first portable device and the second portable device includes a processing device.

16. (Original) The method ac cording to claim 1, further comprising the steps of:

receiving an authenticated system message which includes a command; and

executing the command.

17. (Previously presented) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

providing an application to at least one card of the first and second cards, the application is provided for at least one of:

renewing a security feature of the at least one card, and

updating a security scheme of the at least one card on-chip risk management.

18. (Original) The method ac cording to claim 1, further comprising the step of:

providing a reference point for time to at least one of the first and second portable devices from a central command arrangement.

19. (Original) The method according to the claim 1, further comprising the steps of:

enabling a selective targeting of at least one device of the first and second portable devices; and

applying re-customization procedures on the at least one device.

20. (Original) The method according to the claim 19, further comprising the step of:

selecting a particular response by the at least one device when a predetermined criteria is met.

21. (Original) The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing cryptograms which are related to the first global signing key and the second global signing key.

22. (Original) The method ac cording to claim 20, further comprising the steps of:

generating the cryptograms by one of the first portable device and the second portable device; and

verifying the cryptograms using another one of the first portable device and the second portable device.

23. (Original) The method ac cording to claim 20, wherein the cryptograms are generated by a central authority.

24. (Original) The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, modifying stored parameters of at least one of the first and second cards to at least one of suspend, permit and modify subsequent operations between the first and second cards or other cards.

25. (Currently Amended) A portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following steps:

receiving a second sequence number and a second key from the further portable device, wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

26. (Original) The portable device according to claim 25, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

27. (Original) The portable device according to claim 25, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

28. (Original) The portable device according to claim 25, wherein the storage device stores a third sequence number thereon, and wherein the processing device performs the following:

if the first sequence number and the second sequence number are equal, and

determines whether the third sequence number corresponds to a fourth sequence number of the further portable device.

29. (Original) The portable device according to claim 28, wherein, if the third sequence number corresponds to the fourth sequence number, the processing device performs the transaction with the further portable device.

30. (Original) The portable d evice according to claim 25, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

31. (Original) The portable d evice according to claim 25, wherein the first key is a global signing key, and wherein the second key is a second global signing key.

32. (Currently amended) A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a the first trusted time provided on the first portable device, the second sequence number being indicative of a the second trusted time provided on the second portable device; and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number and conversely,

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

33. (Original) The method ac cording to claim 32, further comprising the step of:

if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number.

34. (Original) The method ac cording to claim 33, further comprising the step of:

after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number.

35. (Original) The method ac cording to claim 34, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the executing step and if the first time is not equal to the second time, performing a transaction between the first card and the second card.

36. (Original) The method ac cording to claim 32, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time is equal to the second time, performing a transaction between the first card and the second card.

37. (Currently amended) A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the further portable device, and

executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number; and conversely,

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

38. (Original) The portable d evice according to claim 37, wherein, if the first time is not equal to the second time, the processing device executes a particular action which is triggered by at least one of the first sequence number and the second sequence number.

39. (Original) The portable d evice according to claim 37,

wherein the portable device is a smart card, and the further portable device is a further smart card, and

wherein, after the execution of the particular action and if the first time is not equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

40. (Original) The portable d evice according to claim 37,

wherein the portable device is a smart card, and the further portable device is a further smart card, and

wherein, if the first time is equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

41. (Currently amended) A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the first portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the second portable device;

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys; and

setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys; and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

42. (Original) The method ac cording to claim 41, further comprising the steps of:

generating the cryptograms by one of the first portable device and the second portable device; and

verifying the cryptograms using another one of the first portable device and the second portable device.

43. (Original) The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key.

44. (Original) The method according to claim 43, wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion.

45. (Original) The method according to claim 43, wherein each of the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys.

46. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, performing a transaction between the first card and the second card.

47. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the verification fails, suspending a transaction between the first card and the second card.

48. (Original) The method according to claim 41, further comprising the step of:

if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device.

49. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time and the second time are equal, performing a transaction between the first card and the second card.

50. (Original) The method ac cording to claim 41,

wherein the first portable device is a first card and the second portable device is a second card,

wherein the setting step is performed by transmitting an authenticated system message command from the second card to the first card, and

wherein at least one of the first and second cards sets the second sequence number.

51. (Original) The method ac cording to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number.

52. (Original) The method ac cording to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device.

53. (Original) The method ac cording to claim 41, wherein each of the first portable device and the second portable device includes a processing device.

54. (Currently amended) A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable

device, the second sequence number being indicative of the second trusted time provided on the further portable device,

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys, and sets the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performs a verification using the first and second keys, and sets the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

55. (Original) The portable d evice according to claim 54, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

56. (Original) The portable device according to claim 54, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

57. (Original) The portable d evice according to claim 54, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

58. (Original) The portable d evice according to claim 54, wherein the first key is a first global signing key and the second key is a second global signing key.